

Supporting Cryptographic Algorithm Agility with Attribute Certificates

Steffen Fries, Rainer Falk

Siemens AG

Technology

Munich, Germany

e-mail: {steffen.fries|rainer.falk}@siemens.com

Abstract—Asymmetric cryptography is broadly used to protect confidentiality, integrity, and authenticity of data during transfer, and potentially also at rest. Typical applications are authentication and key agreement in secure communication protocols, and digital signatures for authentication and integrity protection of documents and messages. These are used in daily life applications like online banking but are specifically used in critical infrastructures to protect against misuse and manipulation. Asymmetric cryptographic algorithms are most often used with digital certificates binding a user identity to a public key of the user. These certificates are used for authentication performed during the handshake by common cryptographic security protocols like Transport Layer Security, Datagram Transport Layer Security, or by authentication and key agreement protocols like the Internet Key Exchange or Group Domain of Interpretation. The cryptographic algorithm for public-key-based user authentication is fixed by the user's certificate. More flexibility to support multiple cryptographic algorithms for user authentication is needed, e.g., by the introduction of new, quantum-safe cryptographic algorithms. Attribute certificates can be used to support flexibly multiple cryptographic algorithms for user authentication, supporting a stepwise transition towards newer cryptographic algorithms.

Keywords—communication security; cryptographic agility; post-quantum cryptography; attribute certificates; industrial automation and control system; Internet of Things; automation control systems.

I. INTRODUCTION

Asymmetric cryptography and digital signatures are a cornerstone in many security architectures. One important application of digital signatures is related to user (entity) authentication and integrity protection of data at rest and in transit. These cryptographic security mechanisms are increasingly used in Critical Infrastructures (CI) to ensure reliable operation. CIs are technical installations that provide essential services for the daily life within a society and the economy of a country. Examples are services in healthcare, telecommunication, transportation, water supply, and power systems. In all types of CIs, a clear trend and also demand towards increased connectivity can be seen. It ensures remote access, but also continuous monitoring to optimize operation and also to support resiliency in case of failures or attacks.

This goes along with a tighter integration of systems from Information Technology (IT) in common enterprise environments with the Operation Technology (OT) part of the automation systems in industrial domains.

There are several differences between IT and OT in terms of security requirements, operational processes, and the lifetime of components used in the related environments. The integration of both domains has mutual influences on the overall security and availability and requires sound security design of interconnected cyber-physical systems.

As stated before, cryptography is one of functions supporting a secure, reliable operation. Cryptographic algorithms typically also underly a lifetime in which they can be treated as secure. Symmetric algorithms are typically designed in a way that they utilize a specific mathematical construct, like a permutation, and depend on the secrecy and/or uniqueness of certain input parameters like a secret key and nonces. Asymmetric cryptographic algorithms are often designed leveraging a specific mathematical problem, in which the calculation in one direction is easy and in the reverse direction the problem solving is computationally hard. These algorithms use two keys, a private key and a public key. Good security design uses public review and does not depend on the secrecy of the underlying mathematical construct.

As outlined in [1], cryptographic algorithms “age”, as the technology to solve certain mathematic problems gets better and better. This can be seen for instance in the availability of increased computational power, e.g., increasingly higher performance processors or available cloud services, to perform brute force attacks to symmetrically encrypted data. Contrary, developments in the area of quantum computers leverage certain physical properties and utilize long-known approaches, which specifically endanger asymmetric cryptographic algorithms [2]. They can solve the previously assumed computationally hard problems much more efficiently. To keep systems secure, also considering the aging of cryptographic algorithms cryptographic agility is required in the system design and operation. This requires support for a migration from currently used cryptographic algorithms to potential new stronger algorithms in the utilized protocols and applications. While this requires considerations in the design, it also requires the flexibility from underlying systems, specifically if cryptographic algorithms are realized in hardware.

This paper focusses on two main points. It provides background information why cryptographic algorithms agility is important from a general requirements point of view, and it addresses specific aspects related to the migration of asymmetric cryptographic algorithms. These algorithms use the construct of public and private keys. Here, a user utilizes his private key for authentication. A peer (relying party) verifies the authentication using the corresponding public key. Digital certificates, e.g., according to the ITU-T X.509 standard [3], confirm the user identity associated with the user’s public key.

Besides entity authentication, digital signatures provide integrity protection of the signed content, which may be a document or, in case of the initial phase of security protocols, protect the negotiation of security parameters for a communication session as used in common security protocols like Transport Layer Security (TLS) [4] and Datagram Transport Layer Security (DTLS) [5], or in “pure” authentication and key agreement protocols like the Internet Key Exchange (IKEv2) [6] or the Group Domain of Interpretation GDOI [7] protocol.

Due to advances in quantum computing, currently used asymmetric cryptographic algorithms like RSA (Rivest, Shamir, Adleman) or ECDSA (Elliptic Curve Digital Signature Algorithm) are endangered, as there underlying mathematical problems, like factorization and discrete logarithm problems (see also [8]) can be solved efficiently using a cryptographically relevant quantum computer leveraging Shor’s algorithm (see also [9]). Symmetric cryptographic algorithms can also be attacked using Grover’s algorithm (see also [9]), but for them it is currently seen sufficient to double the key length without a change of the algorithms (see also [10]).

While the standardization and the journey to introduce new, post-quantum asymmetric algorithms that withstand such attacks is still ongoing, the discussion of transition approaches for currently used cryptographic algorithms to new algorithms has already started (see [11]). In this context, different strategies are being discussed, like the combined or hybrid use of classical and post-quantum algorithms. This also relates to the utilized credentials, which may come in different formats like hybrid certificates supporting alternative cryptographic algorithms in the same certificate (see [1]). However, only a single second public key of a single second cryptographic algorithm can be included. As multiple quantum-safe cryptographic algorithms are currently standardized, a more flexible approach to support multiple public keys for authentication of a single user is needed.

Note that the case of post-quantum cryptographic algorithms is taken here as example. Crypto agility as the ability to adopt to alternative cryptographic algorithms, is a general design objective for protocols and architectures to ensure that new algorithms with similar boundary conditions can be deployed easily.

Transition is specifically important for industrial use cases, as the component lifetime here is much longer compared to consumer electronics. Therefore, it is important to elaborate ways to allow an upgrade of systems already in

the field not only with new algorithms, but also with new or enhanced credentials for entity authentication.

This paper is structured in the following way. Section II provides background on requirements from regulation and standardization to design systems in a way supporting the migration of cryptographic algorithms. Section III sheds light on the topic from a more technical perspective by investigating into related work on cryptographic challenges. Section IV gives an overview on public key certificates and attribute certificates to show the general structure and approach as used in asymmetric cryptographic algorithms. Section V investigates a new approach utilizing attribute certificates to support migration towards stronger cryptographic algorithms. Section VI concludes the paper and provides an outlook to potential future work.

II. FROM REQUIREMENTS TO SOLUTIONS

Security in communication infrastructures is not a new topic. Specifically in office environments or information technology (IT), it is handled as state of the art, and depending on the operational environment certification requirements of specific security processes is mandatory, or at least may provide a competitive advantage.

Critical infrastructures or operational technology (OT) on the other hand also rely on communication and utilize increasingly standard communication protocols or standard components whenever possible. This provides some commonalities regarding the utilized technology for communication, but there are distinct differences in the management and operation of these infrastructures as seen in Figure 1.



	Critical Infrastructures, e.g., Power Systems 	Office IT 
Protection target for security	OT, e.g., generation, transmission	IT- Infrastructure
Component Lifetime	Up to 20 years	3-5 years
Availability requirement	Very high	Medium, delays accepted
Real time requirement	Can be critical	Delays accepted
Physical Security	Very much varying	High (for IT Service Centers)
Application of patches	Slow (in maintenance windows)	Regular / scheduled
Anti-virus	Hard to deploy, white listing	Common / widely used
Security testing / audit	Increasing, partially	Scheduled and mandated

Figure 1. Comparison IT/OT management and operation

These differences in management and operation of the IT systems consequently lead to different high level security requirements as outlined in Figure 2.



	Critical Infrastructures 	Office IT 
Security Awareness	Increasing	High
Security Standards	Under development, regulation	Existing
Confidentiality (Data)	Low – medium	High
Integrity (Data)	High	Medium
Availability / Reliability	24 x 365 x ...	Medium, delays accepted
Non-Repudiation	Medium to High	Medium

Figure 2. Comparison IT/OT high level security requirements

For critical infrastructures, the European Network and Information System (NIS2) Directive [12] requires security measures to be supported by system operators specifically of critical infrastructures. This directive must be ratified by the European member states.

Germany, for instance, has passed the Information technology (IT) Security Act already in 2021 [13], which requires the further definition of domain-specific security measures that have to be implemented by operators of critical infrastructures. For the power system infrastructure, for instance, the domain specific security standard is provided by ISO 27019 [14]. Both documents target communication security in terms of authentication of communicating entities in addition to integrity and confidentiality protection of the data exchange, but without specifying specific technical means in terms of security protocols or specific cryptographic algorithms. Recommendations for the usage of cryptographic algorithms and protocol features of selected security protocols are provided from the German BSI in TR-02102 [15] and maintained on a yearly base.

In addition, the European Cyber Resilience Act (EU-CRA) [16] is currently being finalized. In addition to the NIS2 Directive, the EU-CRA defines specific requirements for manufacturers of devices, which are to be used, beyond others, also in critical infrastructures. The defined requirements relate to different aspects like the product development process, the security provided by the products, based on their features as well as the handling of vulnerabilities, detected while the products are in operation.

These regulative requirements in turn require standards of holistic nature, covering the different aspects from development and production, integration up to the end of lifetime of products. Ideally, these standards will be harmonized across different application domains to ease certification of processes and features.

A standard framework defining specific requirements for operators, integrators, and manufacturers is provided by IEC 62443 [17]. It specifically describes in two distinct parts technical requirements on system and component level, targeting four different security levels, which relate to the strength of a considered attacker. Moreover, this framework also contains requirements regarding the use of cryptographic algorithms including their strength. While ISO 62443 has been written for industrial control systems, it is meanwhile applied in power systems, in the railway industry, but also in not directly related application domains like healthcare.

Security requirements for critical infrastructures are also defined outside Europe, for instance in requirements specified by NIST Cybersecurity Framework [18], which was recently revised to an edition 2. Specifically for the power system infrastructure requirements are posed by the North American Energy Reliability Council in the NERC Critical Infrastructure Protection (CIP) standards [19]. These documents pose similar requirements as the IEC 62443 series, which relate most often to the security processes of an operator and with this direct and indirect requirement to the products used in these environments.

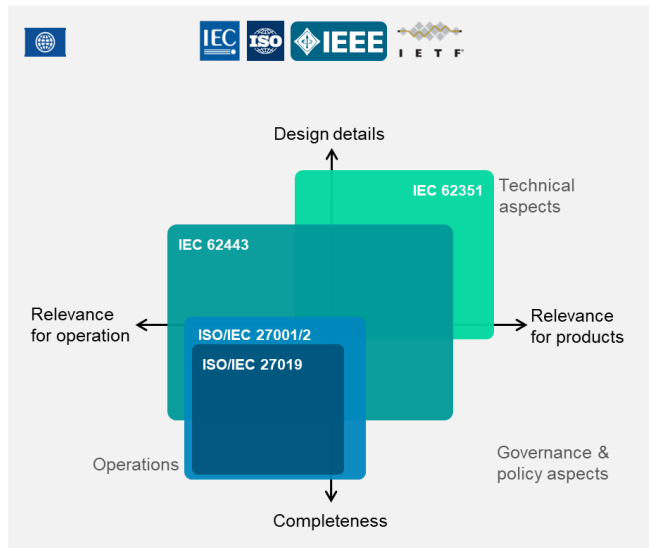
Common to all of the previously stated requirement documents is that they describe requirements on a “what” level, stating the expected security measures, leaving the concrete realization open. Hence, additional standards/specifications are necessary to address the technical implementation of such requirements in components and systems, while ensuring interoperability between different vendor’s products. For the power system infrastructure, this is provided by the IEC 62351 series [20].

The combination of both, procedural and technical security measures provide the necessary support for reliable operation of critical infrastructure systems addressing regulative requirements. This is depicted in Figure 3.

Regulative Requirements



International Standards



Note: the stated organizations and standards are considered the most important for power system automation but are not complete

Figure 3. Relation of Regulative Requirements and Standards on the Example of Power Systems

III. RELATED TECHNICAL WORK

As stated in Section II, there are several requirement sources that point to the ability to update utilized cryptographic algorithms. That this is necessary can be seen on the example of already deprecated cryptographic algorithms, which are no longer considered secure to protect security of sensitive information accordingly. Examples are, for instance, hash functions like MD5 and SHA-1 [21][22], or asymmetric cryptographic algorithms like RSA in key length with less than 2048 bit [15], or symmetric algorithms like DES [15][23].

Quantum computers are investigated since quite a while and advances in the number of supported quantum bits is increasing [24]. Cryptographically relevant quantum computers endanger algorithms like RSA or ECDSA, as their underlying mathematical problems, the factorization problem (for RSA) or the discrete logarithm problem (for ECDSA, see also [8]) can be solved efficiently leveraging Shor's algorithm (see also [9]). Symmetric cryptographic algorithms can also be attacked using Grover's algorithm (see also [9]), but for them, it is currently seen sufficient to double the key length without a change of the algorithms (see also [10]).

To find appropriate cryptographic algorithms that are considered quantum safe, NIST initiated a challenge on replacement algorithms for digital signatures. This challenge is about to finish after six years. Three digital signature candidates have been selected for standardization (see [11]):

- CRYSTALS-Dilithium (ML-DSA, FIPS 204 [28])
- SPHINCS+ (SLH-DSA, FIPS 205 [29])
- FALCON

These algorithms have different parameters and different parameter sizes as the classical algorithms like RSA or ECDSA. The key size can be significantly larger compared to classical cryptographic algorithms. These parameters and key sizes need to be supported by implementations and most importantly also in the context of existing user authentication credentials like X.509 certificates.

The migration or transition to quantum-safe cryptographic algorithms is a complex undertaking. The National Institute for Standards and Technology NIST has published a draft guideline on the migration to post-quantum cryptography [27].

Transition of cryptographic algorithms has been worked on in the context of ITU-T X.509 [3] with the support of alternative cryptographic algorithms as investigated in the following Section IV.A.

With the IETF, a further standardization organization investigates the different options of migration towards post-quantum cryptographic algorithms. Here, the emphasis lies on utilizing hybrid approaches in protocols like TLS [4] or DTLS [5]. Besides integrating new algorithms in cipher suites, also approaches like Key Encapsulation (KEM, [26]) are being discussed to avoid generation of digital signatures on constraint devices.

Besides standardization of general usage protocols, also domain-specific standardization takes the migration to post-quantum cryptography into account. One example is the recent development in the power system related security standardization in the IEC, which currently works on a technical report on the Migration towards stronger cryptographic algorithms in IEC 62351-90-4.

IV. PUBLIC KEY AND ATTRIBUTE CERTIFICATES

X.509 certificates are used for entity authentication and integrity protection. As shown in Figure 4, the concept of a public key certificate is the binding of an entity's identity to a public key, which has a corresponding private key. This private key is kept secret by the entity and can be used to authenticate the entity. The certificate itself is issued by a trusted third party, a certification authority, that digitally signs the certificate. This signature is verified by the relying party as part of certificate path validation to a root certificate.

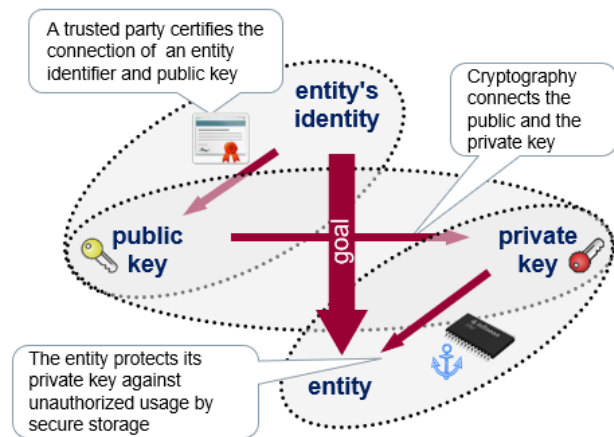


Figure 4. Concept of Binding Public Keys to Identities

These certificates are called public key certificates, as they bind the public key to an entity's identity. In addition, there attribute certificates are defined, which can be seen as temporary enhancement of public key certificates. They do not contain public keys but additional attributes that are connected to the holder of the public key certificate as shown in Figure 5. As visible in the figure, an attribute certificate has a validity period, which may vary based on the application use case. As the attribute certificate can be assumed as a temporary enhancement of a statements contained in a public key certificate, it may be short-lived, or it may have a similar validity as the public key certificate. Figure 5 also shows that the issuing authority may be different for the attribute certificate as for the public key certificate. This fact may be interesting in cases where a separation of duty is targeted.

The following subsections will provide more details on both certificate types.

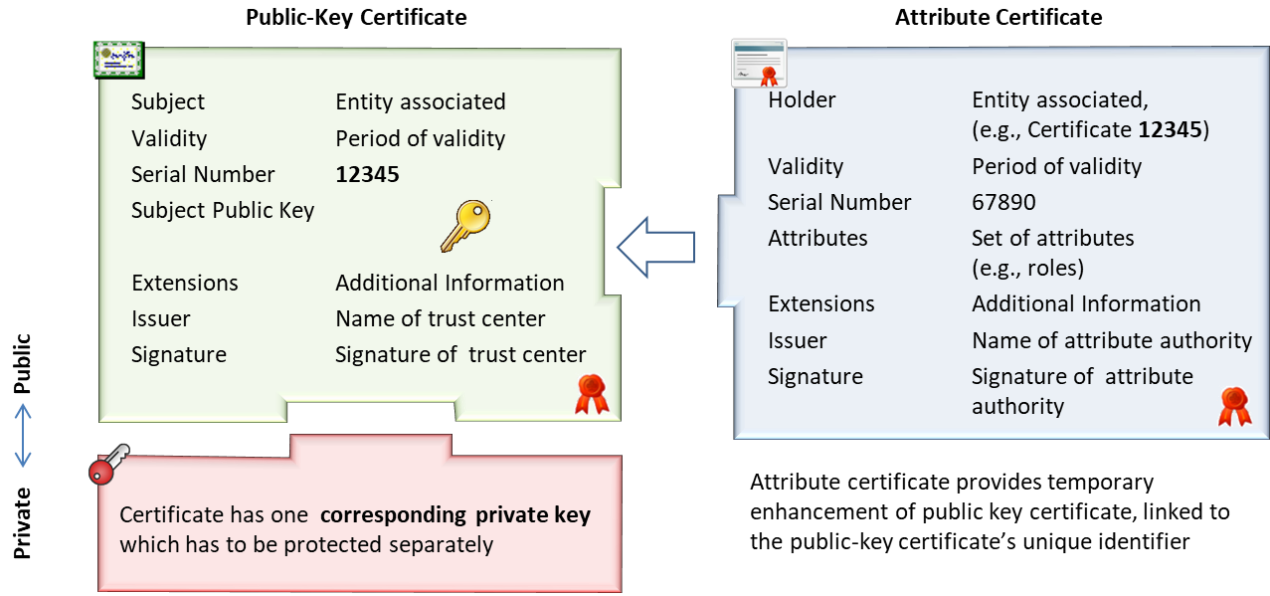


Figure 5. Concept of Public Key Certificates and Attribute Certificates

A. Public Key Certificates

ITU-T X.509 [3] is the public key certificate and attribute certificate framework widely applied in Information Technology (IT) solutions an increasingly being used in Operational Technology (OT) solutions. It defines the structure and content of public key certificates as well as the verification of the components.

```
Certificate ::= SIGNED(TBSCertificate)

TBSCertificate ::= SEQUENCE {
  version                [0] Version DEFAULT v1,
  serialNumber           CertificateSerialNumber,
  signature              AlgorithmIdentifier({SupportedAlgorithms}),
  issuer                 Name,
  validity               Validity,
  subject                Name,
  subjectPublicKeyInfo   SubjectPublicKeyInfo,
  issuerUniqueIdentifier [1] IMPLICIT UniqueIdentifier OPTIONAL,
  ...,
  [[2: -- if present, version shall be v2 or v3
  subjectUniqueIdentifier [2] IMPLICIT UniqueIdentifier OPTIONAL]],
  [[3: -- if present, version shall be v2 or v3
  extensions              [3] Extensions OPTIONAL ]],
  -- If present, version shall be v3]]
} (CONSTRAINED BY { -- shall be DER encoded -- })
```

Figure 6. Public Key Certificate structure (see [1])

As shown in Figure 6, the certificate is a signed structure, containing the subject as the name of the entity and the subjectPublicKeyInfo structure with information about algorithm and the contained public key. The certificate is signed by an issuing certificate authority. Besides further components the certificate structure can also be extended using the extensions component.

To support alternative algorithms, X.509 defines three extensions to convey the:

- subjectAltPublicKeyInfo – alternative public key
- altSignatureAlgorithm – alternative signature algorithm (used to sign the public key certificate) and
- altSignatureValue – alternative signature value.

Using these extensions allows a relying party depending on its capabilities to either utilize classical cryptographic

algorithms or alternative (here post quantum) algorithms for the verification of the certificate (and potential digital signatures performed with the public key corresponding to the contained public key. Depending on the security policy of the relying party, both signatures of the certificate may need to be verified.

This approach is limited to a single alternative key for a public key in practical application, i.e., limited to a single alternative cryptographic algorithm. Simply adding multiple alternative keys to the authentication certificate would increase the certificate size significantly.

B. Attribute Certificates

Besides public key certificates, ITU-T X.509 [1] also defines the structure and content of attribute certificates, as well as the binding to public key certificates and the verification of contained components. Note that besides the binding to public key certificates, an attribute certificate may also be bound to a name of an entity or some fingerprint of information.

An attribute certificate may be seen as temporary enhancement of a public key certificate.

```
AttributeCertificate ::= SIGNED(TBSAttributeCertificate)

TBSAttributeCertificate ::= SEQUENCE {
  version                AttCertVersion, -- version is v2
  holder                 Holder,
  issuer                 AttCertIssuer,
  signature              AlgorithmIdentifier({SupportedAlgorithms}),
  serialNumber           CertificateSerialNumber,
  attrCertValidityPeriod AttCertValidityPeriod,
  attributes             SEQUENCE OF Attribute({SupportedAttributes}),
  issuerUniqueID         UniqueIdentifier OPTIONAL,
  ...,
  extensions             OPTIONAL }

```

Figure 7. Attribute Certificate structure (see [1])

As shown in Figure 7, similar to public key certificates an attribute certificate is also a signed structure, containing the holder as the name of the entity, information about the

issuer, including the signature algorithm and values as well as the possibility to define extensions of the attribute certificate. Like for public key certificates, to support alternative algorithms, X.509 defines two extensions to convey the:

- `altSignatureAlgorithm` – alternative signature algorithm (used to sign the attribute certificate) and
- `altSignatureValue` – alternative signature value.

The standard does not foresee the capability to contain an alternative public key of the holder as additional attribute. The next section discusses the merits of providing this information as well as further, policy related information in the context of an attribute certificate.

V. PROPOSED NEW ATTRIBUTES

As discussed in Section IV, not all extensions defined for public key certificates are defined for inclusion in attribute certificates. This paper therefore proposes to use the `subjectAltPublicKeyInfo` extension also in attribute certificates to convey an alternative public key and information about the corresponding cryptographic algorithms, e.g., a public key for a post quantum asymmetric algorithm like FALCON, DILITHIUM, or SPHINCS+. This allows to associate and utilize alternative public keys to already existing certificates. As multiple attribute certificates can be issued for a single user certificate, implicitly various cryptographic algorithms can be supported in a flexible way by issuing multiple corresponding attribute certificates.

Attribute certificates contain attributes, and providing an alternative public key as attribute is proposed as novel approach. It is intended to support smooth transition to public-key certificates using solely alternative, in the case here, post quantum cryptographic algorithms. As they are intended as temporary enhancement of public key certificates, this approach is seen appropriate. It is even possible to issue attribute certificates for an entity's public key certificate at a later point in time.

For migration to post-quantum cryptography, it is necessary to also support a security policy which handles the transition from one cryptographic algorithm to an alternative cryptographic algorithm (in the case here for digital signatures). Such a policy may require verifying only one signature, both signatures (classic and alternative), and may also provide a weight on the verification result, e.g., by the order of operations. Such a security policy may be configured per relying party. In case of automation networks, it may be part of the engineering data for the Intelligent Electronic Devices (IED).

An alternative approach to the device configuration of security policies is the provisioning of the policy as part of the certificate, also in the form factor of an extensions. This paper proposes such an extension as shown in Figure 8 that may be applied in both certificate types, i.e., to public key certificates as well as to attribute certificates.

```
altCryptoPolicy ::= SEQUENCE {
  combAND    [0] boolean OPTIONAL,
  combOR     [1] boolean OPTIONAL,
  weightOnAlt [2] boolean OPTIONAL
}
```

Figure 8. Proposed Migration Policy Extension

The extension allows to specify the following security policies for the associated alternative public key:

- `combAND` requires the verification of the signature performed with the classic asymmetric algorithm as well as the alternative algorithm.
- `combOR` requires the verification signatures created with of either the classical or the alternative cryptographic algorithm,
- `weightOnAlt` indicates if the alternative algorithm has a higher weight in the evaluation. Note that this can be used in conjunction with `combOR` for the selection of classical or alternative signatures and also for the `combAND` case in cases, in which one signature verification may fail.

The extension may be included in the certificate as critical extension to ensure that it will be evaluated by the relying party. The inclusion into public key certificate can be done to associate a fixed security policy to the two contained public keys. There is also a benefit by placing the extension into an attribute certificate even in cases where the second public key is not contained in the attribute certificate but in the public key certificate. This approach allows to change the security without the need to issue a new public key certificate, enabling dynamic policy changes.

VI. CONCLUSION AND OUTLOOK

This paper provides an overview on the need for a transition from currently used classical cryptographic algorithms to new, alternative cryptographic algorithms from a requirements and standardization point of view, but also from a technical perspective. More specifically, the focus is placed on the use of digital signatures and credentials conveying the public key within X.509 certificates.

In that respect, a novel approach for using alternative asymmetric algorithms in the context of X.509 certificates has been described. It is proposed to support alternative public keys and associated information in attribute certificates, which enhances the application of already defined certificate extensions for public key certificates also for attribute certificates. By this approach, multiple cryptographic algorithms can be supported flexibly by issuing multiple attribute certificates corresponding to the different public keys of a user. Moreover, a further security policy extension is proposed that allows a dynamic adaptation of the security policy for the transition from classic cryptographic algorithms towards alternative, e.g., post quantum algorithms.

The discussed approach is currently in its infancy and needs to be implemented and tested to get practical experience. This is seen as the next consequent step. Due to the use of an already existing extension to transport the alternative public key, further investigation of the transport of algorithm specific parameters is not seen necessary as already considered in the originally defined extension.

Besides the necessity to perform a deeper investigation of the side conditions of this approach and also a proof-of-concept implementation, it is seen necessary to discuss this approach within standardization. This is because most interacting systems are built with products from different manufacturers. Therefore, standardization is necessary to

ensure interoperability of productions developed by different manufacturers.

REFERENCES

- [1] S. Fries and R. Falk, "Using Attribute Certificates to Support Cryptographic Algorithm Flexibility", ICSNC 2023, The Eighteenth International Conference on Systems and Networks Communications, pp. 6-9, 2023 [Online]. Available from: https://www.thinkmind.org/index.php?view=article&articleid=icsnc_2023_1_20_20022 [retrieved: May, 2024]
- [2] Federal Office for Information Security, "Quantum-safe cryptography – fundamentals, current developments and recommendations", 2022, [Online]. Available from: <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf>, [retrieved: February, 2024]
- [3] ITU-T X.509 ISO/IEC 9594-8:2020, Rec. ITU-T X.509 (2019), Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks, [Online]. Available from: <https://www.itu.int/rec/T-REC-X.509-201910-I/en>, [retrieved: May, 2024]
- [4] E. Rescorla, IETF RFC 8446, "Transport Layer Security (TLS) Protocol v1.3", August 2018, [Online]. Available from: <https://tools.ietf.org/html/rfc8446>, [retrieved: August, 2023]
- [5] E. Rescorla, H. Tschofenig, and N. Modadugu, IETF RFC 9147, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", April 2022 [Online]. Available from: <https://datatracker.ietf.org/doc/html/rfc9147>, [retrieved: May, 2024]
- [6] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, and T. Kirvinen., IETF RFC 7296, "Internet Key Exchange Protocol Version 2 (IKEv2)", 2014, [Online]. Available from: <https://datatracker.ietf.org/doc/html/rfc7296>, [retrieved: May, 2024]
- [7] B. Weis, S. Rowles, and T. Hardjono, IETF RFC 6407, "The Group Domain if Interpretation", October 2011, [Online]. Available from: <https://datatracker.ietf.org/doc/html/rfc6407>, [retrieved: May, 2024]
- [8] A. J. Menezes, P. C. v. Oorschot, and S. A. Vanstone, "Handbook of Applied Cryptography", CRC-Press, October 1996, ISBN: 0-8493-8523-7
- [9] D. J. Bernstein, J. Buchmann, and E. Dahmen, "Post-quantum cryptography", Springer, Berlin, 2009. ISBN 978-3-540-88701-0
- [10] L. Cehen et al., NISTIR 8105, "Report on Post-Quantum Cryptography", April 2016, [Online]. Available from: <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf>, [retrieved: May, 2024]
- [11] NIST "PQC Standardization Process: Announcing Four Candidates to be Standardized", July 2022, [Online]. Available from <https://csrc.nist.gov/news/2022/pqc-candidates-to-be-standardized-and-round-4>, [retrieved: May, 2024]
- [12] NIS2 Directive, 2022, [Online]. Available from https://www.bsi.bund.de/EN/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/it_sig.html, [retrieved: February, 2024]
- [13] The German IT Security Act, 2021, [Online]. Available from: <https://eur-lex.europa.eu/eli/dir/2022/2555>, [retrieved: May, 2024]
- [14] ISO 27019: Information technology - Security techniques - Information security controls for the energy utility industry, 2017, [Online]. Available from: <https://www.iso.org/standard/68091.html>, [retrieved: May, 2024]
- [15] BSI TR-02102, "Cryptographic Mechanisms", [Online]. Available from: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html, [retrieved: May, 2024]
- [16] EU Cyber Resilience Act, [online]. Available from: <https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act>, [retrieved: May, 2024]
- [17] IEC 62443, "Industrial Automation and Control System Security", [Online]. Available from: <https://www.iec.ch/blog/understanding-iec-62443>, [retrieved: May, 2024]
- [18] NIST Cybersecurity Framework 2.0, 2024, [Online]. Available from: <https://www.nist.gov/cyberframework>, [retrieved: May, 2024]
- [19] NERC CIP Set of Standards, [Online]. Available from: <https://www.nerc.com/pa/Stand/Pages/Cyber-Security-Permanent.aspx>, [retrieved: May, 2024]
- [20] IEC 62351-x Power systems management and associated information exchange – Data and communication security, [Online]. Available from: <http://iectc57.ucaug.org/wg15public/default.aspx>, [retrieved: May, 2024]
- [21] L. Velvindron, K. Moriarty, and A. Ghedini, IETF RFC 9155, "Deprecating MD5 and SHA-1 Signature Hashes in TLS 1.2 and DTLS 1.2", 2021, [Online]. Available from: <https://datatracker.ietf.org/doc/html/rfc9155>, [retrieved: May, 2024]
- [22] Announcement, "NIST retires SHA-1 Cryptographic Algorithm", 2022, [Online]. Available from: <https://www.nist.gov/news-events/news/2022/12/nist-retires-sha-1-cryptographic-algorithm>, [retrieved: May, 2024]
- [23] NIST SP 800-131Arev.2, "Transitioning the Use of Cryptographic Algorithms and Key Lengths", 2019, [Online]. Available from: <https://csrc.nist.gov/pubs/sp/800/131/a/r2/final>, [retrieved: May, 2024]
- [24] Federal Office for Information Security, "Status of quantum computer development", Version 2.0, 2023, [Online]. Available from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publicationen/Studien/Quantencomputer/Entwicklungsstand_QC_V_2_0.pdf, [retrieved: May, 2024]
- [25] NIST Announcement, "PQC Standardization Process: Announcing Four Candidates to be Standardized", July 2022, [Online]. Available from: <https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4>, [retrieved: May, 2024]
- [26] F. Giacon., F. Heuer, and B. Poettering, "KEM Combiners", 2018, [Online]. Available from: https://doi.org/10.1007/978-3-319-76578-5_7, [retrieved: May, 2024].
- [27] W. Newhouse, M. Souppaya, W. Barker, and C. Brown, "Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography", April 2023, [Online]. Available from: <https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms> [retrieved: May, 2024]
- [28] FIPS 204: "Module-Lattice-Based Digital Signature Standard", 2024, [Online]. Available from: <https://csrc.nist.gov/pubs/fips/204/ipd>, [retrieved: May, 2024].
- [29] FIPS 205: "Stateless Hash-Based Digital Signature Standard", 2024, [Online]. Available from: <https://csrc.nist.gov/pubs/fips/205/ipd>, [retrieved: May, 2024].